ALERT MEMORANDUM

# Perimetro Di Sicurezza Nazionale Cibernetica: Spunti di Riflessione a Seguito del Completamento Della Normativa

Per qualsiasi questione relativa ai temi discussi in questa nota, potete rivolgervi a qualsiasi avvocato del nostro studio con cui siete abitualmente in contatto o agli autori.

**ROMA**
Piazza di Spagna 15
00187 Roma, Italia
T: +39 06 69 52 21

**Andrea Mantovani**
+39 06 6952 2804
amantovani@cgsh.com

**Federica Mammì Borruto**
+39 06 6952 2826
fmammiborruto@cgsh.com

**MILANO**
Via San Paolo 57
20121 Milano, Italia
T: +39 02 72 60 81

**Lorenzo Freddi**
+39 02 7260 8630
lfreddi@cgsh.com

*17 aprile 2023*

Il 10 gennaio 2023, è stata pubblicata in Gazzetta Ufficiale la Determina del 3 gennaio u.s. dell'Agenzia per la Cybersicurezza Nazionale ("**ACN**") recante la tassonomia degli incidenti aventi un impatto sulle reti, sui sistemi informativi e sui servizi informatici diversi dai Beni ICT (così come sotto definiti) che devono essere oggetto di notifica da parte dei soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica (il "**PSNC**" e la "**Determina**")[1].

Il quadro normativo sul PSNC è, quindi, adesso completo, nonostante non siano ancora stati istituiti i laboratori accreditati di prova ("**LAP**") presso cui potranno essere svolti i test disposti dal Centro di Valutazione e Certificazione Nazionale ("**CVCN**").

La pubblicazione della Determina, divenuta efficace il 25 gennaio u.s., rappresenta un'occasione utile per svolgere riflessioni più ampie sul complesso di norme in tema di PSNC. La normativa coinvolge, infatti, non solo i soggetti inclusi nel PSNC, ma anche terzi *provider* di beni e servizi che agiscono sui sistemi di proprietà dei primi. Nello specifico, i *provider,* oltre a essere diretti destinatari di specifici obblighi, devono comunque adeguare la loro offerta agli obblighi a cui sono soggetti i loro clienti inclusi nel PSNC, per consentire a questi ultimi il rispetto delle norme.

Risulta fondamentale, pertanto, che tutti i soggetti a vario titolo coinvolti riflettano sull'attuazione di un modello organizzativo aziendale in materia di cybersicurezza che tenga conto della predetta normativa, definendo i processi potenzialmente impattati e formalizzando misure tecniche e organizzative efficaci per mitigare eventuali rischi.

[1] Art. 1, comma 3-*bis* del D.L. 105/2019.

## I. La normativa sul PSNC

La normativa in tema di PSNC[2] è indirizzata a soggetti nazionali pubblici e privati, individuati con atto amministrativo del Presidente del Consiglio dei Ministri (non soggetto a pubblicazione), in quanto esercitano una funzione o un servizio essenziale o hanno carattere strategico per gli interessi dello Stato e, in particolare, alle reti, ai sistemi informativi e ai servizi informatici di tali soggetti dal cui malfunzionamento, interruzione, anche parziali, o utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale ( i "**Beni ICT**"). L'ACN[3] informa i predetti soggetti dell'avvenuta inclusione nel PSNC, con comunicazione indicante la funzione o il servizio essenziale di pertinenza.

**Obblighi imposti ai soggetti inclusi nel PSNC**

Ai soggetti inclusi nel PSNC sono imposti, fra l'altro, obblighi di:

- predisposizione e trasmissione all'ACN dell'elenco dei Beni ICT;
- adozione di misure di sicurezza per i Beni ICT;
- notifica al CSIRT (Computer Security Incident Response Team) Italia e gestione degli incidenti di sicurezza aventi impatto sui Beni ICT o inclusi nell'allegato A della Determina;
- comunicazione al CVCN e rispetto di apposite procedure per lo scrutinio tecnologico degli approvvigionamenti di *asset* tecnologici rilevanti.

**Trasmissione dell'elenco dei Beni ICT**

I soggetti inclusi nel PSNC devono trasmettere l'elenco dei Beni ICT entro sei mesi dalla data di ricevimento della comunicazione di avvenuto inserimento nel PSNC[4].

L'elenco deve essere aggiornato con cadenza almeno annuale e comunicato all'ACN. Qualora insorgano modifiche sostanziali, l'elenco dei Beni ICT nonché il modello che descrive le misure di sicurezza adottate dai soggetti inclusi nel PSNC devono essere aggiornati e trasmessi all'ACN.

**Misure di sicurezza**

Le misure di sicurezza sono indicate nell'allegato B al DPCM 81/2021 e si distinguono in due categorie (A e B) – a seconda della loro complessità (le misure di sicurezza di categoria B sono quelle più onerose, tra cui rientrano anche i requisiti di localizzazione) – a cui corrispondono diversi tempi di adozione.

Le misure di sicurezza per i Beni ICT sono relative a:

- struttura organizzativa preposta alla gestione della sicurezza;
- politiche di sicurezza e gestione del rischio;
- mitigazione e gestione degli incidenti e loro prevenzione, anche attraverso interventi su apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza;
- protezione fisica e logica e dei dati;
- integrità delle reti e dei sistemi informativi;
- gestione operativa, ivi compresa la continuità del servizio;
- monitoraggio, test e controllo;
- formazione e consapevolezza;
- affidamento di forniture di beni, sistemi e servizi ICT.

[2] Il D.L. 21 settembre 2019, n. 105 (convertito con modificazioni, dalla legge 18 novembre 2019, n. 133) ha istituito il PSNC. La disciplina ha poi avuto diversi decreti attuativi: *(i)* DPCM 30 luglio 2020, n. 131, che ha dettato criteri e modalità per l'individuazione dei soggetti inclusi nel PSNC; *(ii)* DPR 5 febbraio 2021, n. 54, che disciplina i procedimenti di verifica circa le condizioni di sicurezza e l'assenza di vulnerabilità di beni e servizi ICT; DPCM 14 aprile 2021, n. 81, che definisce le modalità per la notifica in caso di incidenti riguardanti Beni ICT; *(iii)* DPCM del 15 giugno 2021, che individua le categorie dei beni, dei sistemi e dei servizi ICT che saranno oggetto di verifica circa le condizioni di sicurezza e l'assenza di vulnerabilità; *(iv)* DPCM del 18 maggio 2022, n. 92, in materia di identificazione delle regole di accreditamento dei laboratori deputati a svolgere la verifica circa le condizioni di sicurezza e l'assenza di vulnerabilità dei beni, sistemi e servizi ICT.

[3] L'ACN, istituita con D.L. n. 82 del 14 giugno 2021 (convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109) ha diverse competenze in relazione al PSNC, avendo assunto tutte le funzioni precedentemente attribuite al Ministero dello sviluppo economico, alla Presidenza del Consiglio dei ministri, al Dipartimento delle Informazioni per la Sicurezza (DIS) e al CVCN nonché le attività di ispezione e verifica e la maggior parte di quelle relative all'accertamento delle violazioni e all'irrogazione delle sanzioni amministrative.

[4] In caso di mancata trasmissione, può essere comminata una sanzione amministrativa pecuniaria da euro 200.000 a euro 1.200.000.

L'ACN può svolgere verifiche e ispezioni per accertare, tra l'altro, se sono state correttamente adottate le misure di sicurezza[5].

**Misure di sicurezza di categoria A**

Devono essere adottate entro sei mesi dalla data di trasmissione degli elenchi dei Beni ICT.

- Esempio: il soggetto incluso nel PSNC deve effettuare una valutazione del rischio (*risk assessment*), che comprende l'identificazione e la documentazione delle vulnerabilità delle risorse.

**Misure di sicurezza di categoria B**

Devono essere adottate entro trenta mesi dalla data di trasmissione degli elenchi dei Beni ICT.

- Esempio: a seguito della valutazione del rischio, deve essere redatto un documento in cui siano descritte le scelte operate in relazione a ciascun rischio individuato e le relative priorità.

**Requisiti di localizzazione[6]**

I requisiti di localizzazione si distinguono a seconda della tipologia di dati trattati:

- Dati digitali trattati mediante impiego di Beni ICT o relativi alla descrizione di tali Beni. Devono essere conservati, elaborati o estratti esclusivamente mediante l'impiego di infrastrutture fisiche e tecnologiche, anche se esternalizzate, localizzate sul territorio nazionale. Tali infrastrutture includono anche quelle deputate alle funzioni di *business continuity*.
- Dati digitali utilizzati dalle infrastrutture deputate alla sicurezza e infrastrutture di *disaster recovery*. Anche se esternalizzati, devono essere localizzati sul territorio nazionale, salvo motivate e documentate ragioni di natura normativa o tecnica. In presenza di tali motivazioni i predetti dati e infrastrutture non devono comunque essere localizzati al di fuori del territorio dell'Unione europea.
- Dati digitali di *backup*. Qualora cifrati, anche se esternalizzati, possono essere conservati al di fuori del territorio nazionale, ma non al di fuori del territorio dell'Unione europea e le chiavi di cifratura devono essere comunque custodite all'interno del territorio nazionale. Le operazioni di cifratura e decifratura devono comunque essere eseguite mediante infrastrutture localizzate sul territorio nazionale.

Questi requisiti di localizzazione sono probabilmente quelli che hanno creato maggiori difficoltà applicative nella prassi, soprattutto perché, sotto il profilo pratico, il loro rispetto può imporre sostanziali ristrutturazioni dell'architettura dei sistemi informatici.

La localizzazione dei dati e delle infrastrutture fisiche e tecnologiche utili al loro trattamento serve ad agevolare:

- la verifica dell'implementazione delle misure di sicurezza anche mediante le ispezioni fisiche in loco da parte dell'autorità italiana;
- in caso di incidenti, la verifica e valutazione delle eventuali cause;
- l'accorciamento della catena di controllo dei dati;
- maggiore flessibilità nella modifica delle misure di sicurezza specifiche.

Si tratta, quindi, di uno strumento finalizzato a rendere controllabile e misurabile la modalità di trattamento dei dati di interesse, agevolando tra l'altro l'interazione tra soggetto controllato e soggetto controllore in presenza di incidenti che mettano a rischio la sicurezza nazionale.

[5] L'inosservanza di tale obbligo è punita con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000.

[6] DPCM del 14 aprile 2021, n. 81, Allegato B, art. 3.3.1 PR.DS-1.

**Notifica degli incidenti di sicurezza**

Quando un soggetto incluso nel PSNC viene a conoscenza di un evento riconducibile a quelli descritti nell'allegato A del DPCM n. 81/2021, deve procedere alla relativa notifica al CSIRT Italia, attraverso appositi canali. È prevista anche una notifica volontaria riguardo a incidenti non dettagliati nella normativa, la quale non può, in ogni caso, avere l'effetto di imporre al soggetto notificante obblighi a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica.

La notifica deve essere effettuata entro sei ore, qualora si tratti di un incidente individuato nella tabella 1 dell'allegato A (ad esempio, evidenza di impiego non autorizzato di tecniche utili a esfiltrare dati dall'interno della rete verso risorse esterne), ed entro un'ora, qualora si tratti di un incidente individuato nella tabella 2 del medesimo allegato (ad esempio, divulgazione non autorizzata di dati digitali relativi ai Beni ICT)[7]. I termini decorrono dal momento in cui i soggetti inclusi nel PSNC vengono a conoscenza dell'incidente.

Quanto agli incidenti, che non riguardano i Beni ICT, riconducibili a una delle categorie indicate nell'allegato A della Determina[8], la notifica è obbligatoria per quanto riguarda gli incidenti ricompresi nelle categorie della Sezione 1 di tale allegato, mentre è volontaria (e può essere effettuata con le stesse modalità previste per quella obbligatoria) per quanto concerne gli incidenti di cui alla Sezione 2. La notifica di questi incidenti deve essere inviata al CSIRT Italia entro 72 ore dal momento in cui il soggetto colpito ne viene a conoscenza, a seguito delle evidenze ottenute anche mediante le attività di monitoraggio, test e controllo.

Al fine di individuare in modo univoco tali termini, fra le misure di sicurezza di cui all'allegato B del DPCM n. 81/2021 è previsto che i soggetti inclusi nel PSNC elaborino un documento recante i ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento degli incidenti con impatto e la loro successiva notifica allo CSIRT Italia nonché elementi volti a rendere tempestiva la rilevazione di tali eventi.

Una volta definiti e avviati i piani di attuazione delle attività per il ripristino dei Beni ICT impattati dall'incidente oggetto di notifica, il soggetto incluso nel PSNC ne dà tempestiva comunicazione al CSIRT Italia e trasmette, altresì, su richiesta del CSIRT Italia ed entro trenta giorni dalla stessa richiesta, una relazione tecnica che illustra gli elementi significativi dell'incidente, tra cui le conseguenze dell'impatto sui Beni ICT derivanti dall'incidente e le azioni intraprese per porvi rimedio, salvo che l'autorità giudiziaria procedente abbia previamente comunicato la sussistenza di specifiche esigenze di segretezza investigativa.

## II. La procedura dinanzi al CVCN

I soggetti inclusi nel PSNC sono tenuti a effettuare una comunicazione al CVCN qualora intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT rientranti nelle categorie individuate dal DPCM 15 giugno 2021, destinati a essere impiegati sui Beni ICT[9].

La comunicazione comprende, fra l'altro, un documento di analisi del rischio associato all'oggetto della fornitura[10].

[7] Il mancato adempimento dell'obbligo di notifica è punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000.

[8] La Determina classifica gli incidenti informatici e le varie fasi dell'attacco in sei categorie (suddivise tra la Sezione 1, per quanto riguarda le categorie accesso iniziale, esecuzione, installazione, movimenti laterali, azioni sugli obiettivi, e la Sezione 2, per quanto riguarda l'attività di *spearphishing*), con indicazione di un codice identificativo per ogni incidente, unitamente alla descrizione di ciascuna tipologia. Gli incidenti catalogati nella Determina comprendono la maggior parte delle tecniche di attacco informatico descritte dal MITRE ATT&CK, un riferimento internazionale per le tecniche e procedure di attacco informatico (accessibile tramite il seguente link).

[9] Art. 1, comma 6 del D.L. n. 105/2019. Tali categorie includono: componenti *hardware* e *software* che svolgono funzionalità e servizi di rete di telecomunicazione (accesso, trasporto, commutazione), ad esempio *router*; componenti *hardware* e *software* che svolgono funzionalità per la sicurezza di reti di telecomunicazione e dei dati da esse trattati, ad esempio *virtual private network* (VPN); componenti *hardware* e *software* per acquisizione dati, monitoraggio, supervisione controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali, ad esempio sistemi di AI e ML per la gestione delle reti o dei sistemi; e applicativi *software* per l'implementazione di meccanismi di sicurezza, ad esempio applicativi di *single sign-on*.

[10] L'impiego di prodotti e servizi sulle reti in violazione delle condizioni o in assenza del superamento dei test imposti dal CVCN è punito con la sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000. Il mancato rispetto delle prescrizioni imposte dal CVCN è, inoltre, punito con la sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000.

**Tempistiche**

- I soggetti inclusi nel PSNC, prima dell'avvio delle procedure di affidamento o della conclusione dei contratti relativi alla fornitura di beni, sistemi e servizi ICT, ne danno comunicazione al CVCN.
- A partire dalla data della notifica, il CVCN ha un termine di quarantacinque giorni (prorogabile una sola volta di quindici giorni in casi di particolare complessità) per effettuare verifiche preliminari ed eventualmente richiedere informazioni.
- Un successivo termine (di sessanta giorni) è previsto per l'esecuzione di test disposti dal CVCN all'esito delle verifiche preliminari e decorre dal momento in cui, avendo il CVCN disposto che i test debbano essere eseguiti, il soggetto incluso nel PSNC comunica che l'oggetto della valutazione è reso fisicamente disponibile per tali test.
- I termini del procedimento possono essere sospesi ove il CVCN chieda informazioni al soggetto incluso nel PSNC e vi sia incompletezza o incongruenza delle informazioni fornite o in caso di malfunzionamento dell'oggetto di valutazione o dell'ambiente di test predisposto dal fornitore, che renda impossibile o difficoltosa l'esecuzione dei test.

I test che il CVCN può disporre sono:

- test di corretta implementazione delle funzionalità di sicurezza allo scopo di verificare che queste ultime si comportino secondo le relative specifiche di progetto;
- test di intrusione a supporto dell'analisi di vulnerabilità.

Il CVCN può imporre il rispetto di specifiche condizioni e test da eseguire e può imporre ulteriori requisiti relativi al supporto che il *provider* deve prestare, nonché, a questo proposito, imporre di apportare modifiche al contratto tra il *provider* e il soggetto incluso nel PSNC, affinché il contratto sia condizionato al rispetto dei requisiti e all'esito favorevole dei test[11].

È importante che siano gestite contrattualmente (ad esempio tramite condizioni sospensive e/o impegni a recepire nel contratto le modifiche richieste) le tempistiche del procedimento dinanzi al CVCN. Questo perché la comunicazione al CVCN deve avvenire, secondo la norma, "*prima della conclusione dei contratti*", ma la tempistica del procedimento non è del tutto prevedibile.

## III. Obblighi a carico dei *provider*

Esistono specifici obblighi a carico del *provider* che fornisca beni o servizi rilevanti a soggetti inclusi nel PSNC.

Con riguardo all'implementazione delle misure di sicurezza da parte dei soggetti inclusi nel PSNC, il *provider* deve:

- consentire al soggetto incluso nel PSNC di valutare la sua affidabilità tecnica sulla base di un processo di valutazione del rischio inerente la catena di approvvigionamento *cyber* (tra cui la qualità dei prodotti e delle pratiche di *cybersecurity*, la capacità di garantire l'approvvigionamento, l'assistenza e la manutenzione nel tempo, la disponibilità a condividere il codice sorgente, l'esistenza di certificazioni o evidenze utili a valutare la qualità del processo di sviluppo del *software*, l'implementazione di procedure e strumenti tecnici per garantire l'autenticità e l'integrità del *software* o del *firmware* installato nei Beni ICT e l'implementazione di procedure e strumenti tecnici per garantire una corrispondenza univoca tra il codice sorgente e il codice oggetto installato ed eseguito all'interno dei Beni ICT);

[11] Art. 5, comma 6, del DPR 5 febbraio 2021, n. 54.

- implementare misure appropriate volte a soddisfare gli obiettivi del programma di *cybersecurity* e del piano di gestione del rischio relativo alla catena di approvvigionamento *cyber* adottato dal soggetto incluso nel PSNC;
- consentire al soggetto incluso nel PSNC di effettuare *audit*, verifiche o altre forme di valutazione periodica per confermare l'adempimento degli obblighi contrattuali.

Anche in relazione alla procedura dinanzi al CVCN, la normativa prevede specifici obblighi a carico dei *provider*:

- fornire al CVCN evidenza dell'idoneità delle funzioni di sicurezza e delle loro configurazioni a soddisfare i requisiti di sicurezza;
- allestire un ambiente di *test* presso un LAP o, se necessario, presso la sede del fornitore o del soggetto incluso nel PSNC;
- fornire una descrizione generale dell'architettura dei servizi, beni o sistemi ICT oggetto di valutazione e delle loro funzioni;
- fornire una descrizione delle funzionalità di sicurezza implementate con riguardo i servizi, beni o sistemi ICT oggetto di valutazione;
- fornire una descrizione dei *test* funzionali e di sicurezza già eseguiti, comprensivi dei relativi risultati;
- collaborare con il CVCN nell'esecuzione dei test e attivarsi per risolvere eventuali malfunzionamenti.

I costi per le attività di valutazione svolte dal CVCN, nonché per le attività di test condotte dai LAP, sono a carico del *provider*.

**Obblighi contrattuali**

I contratti conclusi con i *provider* che forniscono beni o servizi rilevanti a soggetti inclusi nel PSNC possono disciplinare ulteriori aspetti quali, ad esempio, tempistiche e modalità:

- con cui il soggetto incluso nel PSNC effettua attività di *audit* nei confronti del *provider*;
- di comunicazione fra le parti in caso di incidenti di sicurezza.

## IV. Conclusioni

Il PSNC deve essere immaginato come un quadro normativo dinamico, in costante aggiornamento a causa della rapida evoluzione dei rischi cibernetici, sia per quanto riguarda gli obblighi a carico dei soggetti inclusi nel PSNC, in particolare con riguardo alle misure di sicurezza, sia in relazione allo stesso elenco dei soggetti inclusi.

Inoltre, questa normativa assume particolare rilevanza anche per i *provider* di beni e servizi che, pur non essendo inclusi nel PSNC, sono destinatari diretti di alcuni specifici obblighi e devono adeguare la propria offerta agli obblighi a cui sono soggetti i loro clienti inclusi nel PSNC.

…

CLEARY GOTTLIEB